

Computing all elliptic curves over an arbitrary number field with prescribed primes of bad reduction

Angelos Koutsianas

Abstract

In this paper we study the problem of how to determine all elliptic curves defined over an arbitrary number field K with good reduction outside a given finite set of primes S of K by solving S -unit equations. We give examples of elliptic curves over \mathbb{Q} and quadratic fields.

1 Introduction

Let K be a number field and S a finite set of primes (non-archimedean) of K . By a classical result of Shafarevich (see [Sil08]) we know that there are finitely many isomorphism classes of elliptic curves defined over K with good reduction at all primes outside S . Many people have previously discovered methods to find explicit representatives of each isomorphism class ([CL07], [Kid01a], [Kid01b]). It is not hard to show (see [CL07]) that it is enough to determine the j -invariants of the isomorphic classes and from them we can easily determine the elliptic curves. In the Cremona–Lingham method, given in [CL07], the j -invariants are found by computing S -integral points on specific elliptic curves. However, the available method of finding S -integral on an elliptic curve requires the Mordell–Weil group of the curve and that problem may be really hard.

The new idea¹, which we display here, is to find the possible j -invariant indirectly using the Legendre λ -invariant. They are related by,

$$j = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(1 - \lambda)^2} \quad (1)$$

and we know that λ lies in the 2-division field L of the associated elliptic curve. Such a field L is a Galois extension of K with $\text{Gal}(L/K)$ isomorphic to a subgroup of S_3 and unramified outside $S^{(2)} = S \cup \{\mathfrak{p} \subset \mathcal{O}_K : \mathfrak{p} \mid 2\}$. We will first prove that there are only finitely many extensions L with these two properties and will give an algorithm for determining all of them. If S_L is the set of all primes in L which are above the primes of $S^{(2)}$, then we know that λ is in \mathcal{O}_{L,S_L}^* , the group of the S_L -units of L . In addition, $\mu = 1 - \lambda$ is related to the same j and lies in \mathcal{O}_{L,S_L}^* hence as well. So, we have that a possible λ with respect to j satisfies the equation:

$$\lambda + \mu = 1 \quad (2)$$

¹Suggested to John Cremona in a personal communication with Noam Elkies in June 2010.

where $\lambda, \mu \in \mathcal{O}_{L, S_L}^*$. Solving the above equation for each L/K we find all λ . Then we determine the j -invariants of the elliptic curves we are seeking and from these it is easy to find the elliptic curves (see [CL07, §3]).

The above equation (2) is a special case of the general family of Diophantine equations which are called S -unit equations [Sma98]. By the theory of linear forms in logarithms and Siegel's theorem ([Sil08]) we know that such a Diophantine equation has a finite set of solutions. During the 1980's and 1990's many methods of solving S -unit equations algorithmically were developed. De Weger in his thesis and an article ([Weg88], [Weg87]) gave an algorithmic solution for the special case when $K = \mathbb{Q}$ using lattice basis reduction algorithms. Many others used and extended De Weger's idea to solve S -unit equations over an arbitrary number field ([TW89], [Sma95], [TW92], [Sma98]). However, when the degree of the number field or the set of primes S is large then the final sieve step of the method may not be efficient. For this reason, a new idea was introduced by Wildanger and was extended by Smart ([Wil00], [Sma99]) which improves the practicality of solving the S -unit equation (2).

Using the above algorithmic methods, how to solve the S -unit equation (2), unable us to find all λ . Thus, the new algorithm we suggest has three main parts which are the following, given K and S as input:

- Find the finite set of all possible 2-division fields L/K where λ may lie.
- For each extension L/K solve the related S -unit equation $\lambda + \mu = 1$ only for λ and μ such that the associated $j \in K$.
- For each λ we evaluate j and then we find the elliptic curves.

Even though our algorithm is based on the above general algorithmic methods for solving S -unit equations in L , we will be able to derive additional conditions on λ . The main such additional condition is simply that we may also assume that the value of j (obtained from λ via (1)) lies in K ; this restricts λ to lie in a subgroup of \mathcal{O}_{L, S_L}^* of substantially smaller rank.

This paper has five sections. In the first we fix some of the notation and describe the basic properties of the 2-division field. In the second section we describe how we can compute the set of all possible 2-division fields L/K using Kummer theory and we prove that there are finitely many of these. In the third section we give necessary and sufficient conditions of λ to be at the same time a solution of the S -unit equation (2) and the λ -invariant of an elliptic curve defined over K . These conditions make the algorithmic methods of solving equation (2) more effective by allowing us to replace the finitely generated group \mathcal{O}_{L, S_L}^* with one subgroup of smaller rank. We also explain how we can reduce the number of S -unit equations we have to solve. In the fourth section we show how we can modify Smart and Windanger's ideas in order to speed up the sieve step in the solution of (2). In the final section we give examples of elliptic curves in the case when $K = \mathbb{Q}$ or a quadratic field, and we compare our method with current implementations.

Unfortunately, as far as we know there is no implementation in any known software package (Sage, Magma etc) that solves general S -unit equations. Since our new method is based on the algorithmic solution of S -unit equations we had to implement

such an algorithm. The importance of an effective implementation of solving general S -unit equations is not limited to our problem, but may be applied to many other problems in Number Theory and Diophantine equations. We stress that it is not trivial at all to implement such an algorithm.

Acknowledgements: I would to thank my supervisor professor John Cremona for suggesting me this problem, for the long discussions we had and his constant encouragement. Also, for the suggestion of Proposition (4.4) and his comments on an earlier draft of this article. Moreover, I want to thank ICERM and Brown University because a big part of the paper was written during my visit in the institute. Finally, I would like to thank Bekiari-Vekri foundation and the Academy of Athens for funding a part of my studies and EPSRC for covering a part of my fees.

2 Notation–Basic definitions

Let K be a number field and S a finite set of primes of K . Let E be an elliptic curve over K in the long Weierstrass form

$$E : y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6$$

which has good reduction outside the set S . Let j be the j -invariant of the curve and Δ its discriminant.

We define the ring of S -integers $\mathcal{O}_{K,S}$ of K , the S -unit group $\mathcal{O}_{K,S}^*$ of K^* and the n -Selmer group of K and S to be

$$\begin{aligned} \mathcal{O}_{K,S} &= \{x \in K^* \mid \text{ord}_{\mathfrak{p}}(x) \geq 0, \forall \mathfrak{p} \notin S\} \\ \mathcal{O}_{K,S}^* &= \{x \in K^* \mid \text{ord}_{\mathfrak{p}}(x) = 0, \forall \mathfrak{p} \notin S\}. \\ K(S, n) &= \{x \in K^*/K^{*n} \mid \text{ord}_{\mathfrak{p}}(x) \equiv 0 \pmod{n}, \forall \mathfrak{p} \notin S\} \end{aligned}$$

It is known that $\mathcal{O}_{K,S}^*$ is a finitely generated abelian group and $K(S, n)$ a finite abelian group (see [Coh99]). For $n \mid m$ we define $K(S, n)_m$ to be the image of the natural map $K(S, m) \rightarrow K(S, n)$. For a positive natural number n we also define

$$S^{(n)} = S \cup \{\mathfrak{p} \mid \text{ord}_{\mathfrak{p}}(n) > 0\}.$$

In order to determine all elliptic curves E/K with good reduction outside S it is enough to determine the j -invariants of the isomorphic classes of the curves ([CL07]). The cases $j = 0$ and $j = 1728$ were treated fully in [CL07] and so we omit these from consideration throughout this paper. For other j we have the following,

Proposition 2.1 ([CL07]). *Let E be an elliptic curve defined over K with good reduction at all primes $\mathfrak{p} \notin S$ and $j \neq 0, 1728$. Set $w := j^2(j - 1728)^3$. Then*

$$\Delta \in K(S, 12), \quad j \in \mathcal{O}_{K,S}, \quad w \in K(S, 6)_{12}.$$

Conversely, if $j \in \mathcal{O}_{K,S}$ with $w \in K(S, 6)_{12}$ then there exists elliptic curve E with $j(E) = j$ and good reduction outside $S^{(6)}$.

An explicit equation of the curve E whose existence is claimed in the above proposition is the following,

$$E : y^2 = x^3 - 3u^2j(j - 1728)x - 2u^3j(j - 1728)^2$$

with $u \in K^*$ is such that $(3u)^6w \in K(S, 12)$. It is shown in [CL07] that this curve has good reduction outside $S^{(6)}$. The other curves with good reduction outside S and the same j -invariant are all twists $E^{(u)}$ of E by $u \in K(S, 2)$.

Recall that the 2-division polynomial of E is defined by,

$$f_2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

where $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$ and $b_6 = a_3^2 + 4a_6$. Denote the roots of f_2 by e_1, e_2, e_3 then the 2-division field of E is $L = K(e_1, e_2, e_3)$.

Definition 2.1. *The λ -invariant of E is,*

$$\lambda = \frac{e_1 - e_3}{e_1 - e_2}.$$

As it stands λ is not well-defined since the numbering of the e_i is not fixed. We use λ to denote any of the six values of the set,

$$\Lambda := \left\{ \lambda, 1 - \lambda, \frac{1}{\lambda}, \frac{1}{1 - \lambda}, 1 - \frac{1}{\lambda}, \frac{\lambda}{\lambda - 1} \right\}$$

We define $\mu := 1 - \lambda$. As we already mentioned in the introduction we have,

$$j = 2^8 \frac{(\lambda(\lambda - 1) + 1)^3}{\lambda^2(1 - \lambda)^2}.$$

An easy calculation shows that any element of the set Λ gives the same j .

Since, L is the splitting field of f_2 then L/K is a Galois extension and its Galois group $\text{Gal}(L/K)$ is isomorphic to a subgroup of S_3 . Moreover, since $\Delta(2^4f_2) = k^2\Delta(L/K)$ for some $k \in \mathcal{O}_K$ and

$$2^4\Delta = \Delta(f_2) = 2^8 \prod_{1 \leq i < j \leq 3} (e_i - e_j)^2 \quad (3)$$

we see that $\mathfrak{p} \nmid 2\Delta \Rightarrow \mathfrak{p} \nmid \Delta(L/K)$. Also, we observe that $L = K(\lambda)$. We summarize the situation in the following proposition,

Proposition 2.2. *The 2-division field L of E is a Galois extension over K unramified at all primes not in $S^{(2)}$, and has Galois group isomorphic to a subgroup of S_3 .*

If $S_L := \{\mathfrak{B} \subset \mathcal{O}_L : \mathfrak{B} \mid \mathfrak{p}, \text{ for some } \mathfrak{p} \in S^{(2)}\}$, then by the above equation (3) we deduce that all $e_i - e_j$ are not divisible by primes not in S_L , and so they are S_L -units. As a result, λ and μ are both S_L -units and are solutions of the S -unit equation (2) over the 2-division field L for the set of primes S_L .

For an extension N/M and a set S_N of prime ideals of N we define

$$\begin{aligned}\mathcal{O}_{N,M,S_N,1}^* &:= \{x \in \mathcal{O}_{N,S_N}^* \mid \text{Norm}_{N/M}(x) = 1\} \\ \mathcal{O}_{N,M,S_N,\pm 1}^* &:= \{x \in \mathcal{O}_{N,S_N}^* \mid \text{Norm}_{N/M}(x) = \pm 1\}\end{aligned}$$

Finally, for a place \mathfrak{p} we define its absolute value to be,

$$|x|_{\mathfrak{p}} = \begin{cases} p^{-f_{\mathfrak{p}} \text{ord}_{\mathfrak{p}}(x)}, & \text{if } \mathfrak{p} \text{ is a finite prime.} \\ |\sigma_{\mathfrak{p}}(x)|, & \text{if } \mathfrak{p} \text{ is a real place.} \\ |\sigma_{\mathfrak{p}}(x)|^2, & \text{if } \mathfrak{p} \text{ is a complex place.} \end{cases}$$

where for \mathfrak{p} an infinite place, $\sigma_{\mathfrak{p}}$ denotes the associated embedding into \mathbb{R} or \mathbb{C} , and $f_{\mathfrak{p}}$ its residual degree when \mathfrak{p} is an finite prime.

3 Computation of 2-Division Fields

Let K be a number field and S a finite set of primes K . We are looking for Galois extensions of K with $\text{Gal}(L/K)$ isomorphic to a subgroup of S_3 . Since S_3 is a solvable group we can construct L/K as a tower of cyclic extensions. We use Kummer theory to construct cyclic extensions even though there are other methods². A detailed description of Kummer theory with a computational point of view and all proofs of the theorems we use can be found in [Coh99] and [Coh96].

Since a cyclic extension is a tower of prime extensions, we focus only on prime degree extensions. By Kummer theory we have,

Proposition 3.1. *Let K be a number field, p a natural prime number such that $\zeta_p \in K$ and S a finite set of primes K . Let $L = K(\sqrt[p]{a})$ with $a \in K/K^{*p}$; if L/K is unramified at all the primes $\mathfrak{p} \notin S$, then $a \in K(S, p)$.*

In case p is an odd prime and $\zeta_p \notin K$ we have to work with the extension $K_z = K(\zeta_p)$. We first focus on $p = 3$ because we are able to give a simple defining polynomial of the extension. We define $S_{K_z} = \{\mathfrak{B} \subseteq \mathcal{O}_{K_z} \mid \exists \mathfrak{p} \in S \text{ s.t. } \mathfrak{B}|\mathfrak{p}\}$. Then we have:

Proposition 3.2. *Let K be a number, $\zeta_3 \notin K$ and S a finite set of prime ideals of \mathcal{O}_K . Let L/K be a Galois 3 degree extension which is unramified at all primes outside S . Then there exists $a \in K_z(S_{K_z}, 3)$ such that $N_{K_z/K}(a) = \beta^3$ for $\beta \in K$ and $L = K(\theta)$ with θ a root of the polynomial $f(x) = x^3 - 3\beta x - \text{Tr}_{K_z/K}(a)$.*

By Propositions 3.1 and 3.2 we know how to construct all the Galois C_2 and C_3 extensions of a number field K which are unramified outside a finite set S of prime ideals of K . For the S_3 case we use the fact that S_3 is a solvable group and a tower of a quadratic and cubic extensions. Even though we care about S_3 extensions in the rest of the section we describe an algorithm of constructing dihedral extensions D_p with p an odd prime $p \equiv 3 \pmod{4}$.

²Class Field theory can also be used for constructing cyclic extensions with the desired properties. See [Coh99] for a detailed description.

Let $K \subset M \subset L$ be a tower of Galois extensions where $\text{Gal}(M/K) \simeq C_2$ and $\text{Gal}(L/M) \simeq C_p$ with p be an odd prime $p \equiv 3 \pmod{4}$. The details of computing general C_p extensions can be found in [Coh99]. We fix the notation such that $\text{Gal}(L/M) = \langle \sigma \rangle$, $\text{Gal}(M/K) = \langle \tau \rangle$, $f(x) \in M[x]$ is a defining polynomial of L/M with the coefficient of x^{p-1} to be 0, $f^\tau = \tau(f)$ and L^τ is the splitting field of f^τ . We use the same notation for lifts of τ and σ to the absolute Galois group $\text{Gal}(\bar{K}/K)$.

Proposition 3.3. *We have that L^τ/M is a Galois C_p extension.*

Proof. Clear. □

Theorem 3.1. *The extension L/K is Galois if and only if $L = L^\tau$.*

Proof. Clear. □

Now we assume that L/K is Galois. The group $\text{Gal}(L/K)$ acts on the roots of f as a subgroup of S_p . Since $p \equiv 3 \pmod{4}$ we know that C_p is a subgroup of the alternative group A_p but D_p is not. The goal is to find an irreducible polynomial h of degree p over K with splitting field $K(h)$ a subfield of L . Considering discriminants, we are able to check the case $\text{Gal}(K(h)/K) = C_p$ and as a result to distinguish³ $\text{Gal}(L/K) = D_p$ and C_{2p} .

For the special case $f = f^\tau$ (i.e. $f \in K[x]$) we have:

Lemma 3.1. *Let f be a defining polynomial of L/M with $f \in K[x]$. Then $\Delta(f) \in K^* \setminus K^{*2}$ if and only if $\text{Gal}(L/K) \simeq D_p$.*

Proof. Let $K(f)$ be the splitting field of f over K . Since L/K is Galois and f a defining polynomial of L/M we have $K \subset K(f) \subset L$. Then $\Delta(f) \in K^{*2} \Leftrightarrow \text{Gal}(K(f)/K) = C_p \Leftrightarrow \text{Gal}(L/K) = C_{2p}$. □

Now we assume that $f \neq f^\tau$. We use the roots of f and f^τ to define a polynomial $h \in K[x]$ of degree p whose splitting field is L . Write $f(x) = (x-a_1)(x-a_2)\cdots(x-a_p)$ and $f^\tau(x) = (x-b_1)(x-b_2)\cdots(x-b_p)$ with $a_i, b_j \in L$.

In case $\text{Gal}(L/K) = D_p$ we may assume that σ permutes the roots a_i and b_j as $\sigma = (a_1 a_2 \cdots a_p)(b_1 b_2 \cdots b_p)$. Also we may assume that $\tau(a_1) = b_1$ and $\tau\sigma\tau = \sigma^{-1}$. Then by induction we get that $\tau(a_i) = b_{p+2-i \pmod{p}}$ for $i = 1, \dots, p$. We define h to be,

$$\begin{aligned} h(x) &= (x - a_1 - b_1)(x - a_2 - b_2) \cdots (x - a_p - b_p) \\ &= (x - a_1 - \sigma(a_1))(x - a_2 - \sigma(a_2)) \cdots (x - a_p - \sigma(a_p)) \end{aligned} \tag{4}$$

with⁴ $a_1 + b_1 \neq 0$. We can easily check that $\tau(h) = h$ and $\sigma(h) = h$, so $h \in K[x]$. We recall that we have assumed that the coefficient of x^{p-1} of f is equal to 0.

Lemma 3.2. *If h and f are as above then h is irreducible in $K[x]$ and $K \subset K(h) \subset L$.*

³ D_p does not have a normal subgroup of order 2 while C_{2p} has one.

⁴If $a_1 + b_1 = 0$ then $a_1 + b_2 \neq 0$ since $b_1 \neq b_2$. So we can change $h(x)$ with $h'(x) = (x - a_1 - \sigma(b_1))(x - a_2 - \sigma(b_2)) \cdots (x - a_p - \sigma(b_p))$.

Proof. The fact that $K \subset K(h) \subset L$ comes from the definition of h and the fact that L/K is Galois.

Let assume that h is not irreducible in $K[x]$. Since $K \subset K(h) \subset L$, $[L : K] = 2p$ and the degree of h is p we conclude that h has a root in K . Without loss of generality we assume that $a_1 + b_1 = \delta \in K$. Applying σ to δ we have $a_1 + b_1 = a_2 + b_2 = \dots a_p + b_p = \delta$. Since the coefficient of x^{p-1} in f is equal to 0 we have that $a_1 + a_2 \dots + a_p = b_1 + b_2 + \dots + b_p = 0$ which means $(a_1 + b_1) + (a_2 + b_2) \dots + (a_p + b_p) = 0 \Rightarrow p\delta = 0$ and we get $\delta = 0$. So, we have $a_1 + b_1 = 0$, contradiction. \square

We summarize the previous results in the following theorem,

Theorem 3.2. *Let L/K be a Galois extension of degree $2p$ for $p \equiv 3 \pmod{4}$ and M its quadratic subfield. Let $\tau \in \text{Gal}(L/K)$ be an element of order 2, $f \in M[x]$ a defining polynomial of L/M such that the coefficient of x^{p-1} is zero, $f^\tau = \tau(f)$ and h as in (4). Then we have,*

- (i) *If $f = f^\tau$ then $\Delta(f) \in K^* \setminus K^{*2}$ if and only if $\text{Gal}(L/K) \simeq D_p$.*
- (ii) *If $f \neq f^\tau$ then h is irreducible and $h \in K[x]$. Moreover, $\Delta(h) \in K^* \setminus K^{*2}$ if and only if $\text{Gal}(L/K) \simeq D_p$.*

Since the p -Selmer group of any number field with respect to any finite set of primes S is a finite abelian group, we can deduce now the following,

Theorem 3.3. *Let K be a number field, S a finite set of prime of K . Then the number of Galois extensions L/K unramified outside S with Galois group equal to C_2 , C_3 or S_3 is finite.*

Now we have all the ingredients to construct all possible 2-division fields of the elliptic curves we are looking for. Propositions 3.1 and 3.2 explain how to get the 2-division fields with Galois group C_2 or C_3 . Using the same propositions we construct all extensions L/K with degree 6 and unramified outside S . By Theorems 3.1 and 3.2 we can understand which of these extensions are Galois with Galois group isomorphic to S_3 .

4 Solving S -unit equations

We recall that K is a number field, S a finite set of prime ideals of K , E is an elliptic curve over K with good reduction outside S , λ is the λ -invariant of E and $\mu = 1 - \lambda$, L is the 2-division field of E , $S_L = \{\mathfrak{P} \subset \mathcal{O}_L : \mathfrak{P} \mid \mathfrak{p}, \text{ for some } \mathfrak{p} \in S^{(2)}\}$ and \mathcal{O}_{L,S_L}^* the S -unit group of L with respect to S_L .

In this section we show that λ and μ lie in a smaller subgroup than the full \mathcal{O}_{L,S_L}^* . That speeds up both the second and third steps of the algorithm. We will not present the algorithmic methods of solving a general S -unit equation since this has been described fully elsewhere as we have already mentioned ([Weg88], [Weg87], [TW89], [TW91], [TW92], [Sma95], [Sma99], [Wil00], [Sma98]).

The group $\text{PGL}_2(\mathbb{Z})$ acts on K with the usual way,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}$$

for $z \in K$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{Z})$.

Since we have assumed that $j \neq 0, 1728$, by equation (1) we see that all the elements of Λ are distinct. We define

$$T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, R = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{Z})$$

where T has order 2 and R has order 3. If $G := \langle T, R \rangle \simeq S_3$ then G acts on Λ . Actually, G acts as a permutation group on the roots of the polynomial⁵ $F_j(x) = \prod_{\lambda' \in \Lambda} (x - \lambda') = (x^2 - x + 1)^3 - \frac{j}{28}x^2(1 - x)^2 \in K[x]$. Because $L = K(\lambda)$ the splitting field of $F_j(x)$ is L . From the above we can see that $\mathrm{Gal}(L/K)$ acts on the set Λ in the same way as a subgroup of G .

We divide into cases, according to the structure of $\mathrm{Gal}(L/K)$.

4.1 $\mathrm{Gal}(L/K)$ is trivial

When $\mathrm{Gal}(L/K)$ is trivial the elliptic curve has full 2-torsion and $\lambda, \mu \in K$. We have to solve (2) for $\lambda, \mu \in \mathcal{O}_{K,S^{(2)}}^*$.

4.2 $\mathrm{Gal}(L/K) \simeq C_2$

In case $\mathrm{Gal}(L/K) \simeq C_2$, the following theorem holds,

Theorem 4.1. *Suppose that $\Lambda \subset \mathcal{O}_{L,S_L}^*$ is associated with an elliptic curve defined over K . Then there exists $\lambda \in \Lambda$ such that $\lambda \in \mathcal{O}_{L,K,S_L,1}^*$.*

Conversely, let $\lambda \in \mathcal{O}_{L,S_L}^$ and j, w, μ as above. If $\mu \in \mathcal{O}_{L,S_L}^*$ and $\lambda \in \mathcal{O}_{L,K,S_L,1}^*$ then $j \in \mathcal{O}_{K,S}$. Moreover, if $w \in K(S, 6)_{12}$ then j is the j -invariant of an elliptic curve with good reduction outside $S^{(6)}$.*

Proof. If τ is a generator of $\mathrm{Gal}(L/K)$ then we can choose $\lambda \in \Lambda$ from the compatibility of the action of G and $\mathrm{Gal}(L/K)$ on the set Λ such that $\tau(\lambda) = T \cdot \lambda = \frac{1}{\lambda}$. As a result,

$$N_{L/K}(\lambda) = 1.$$

Conversely, if $N_{L/K}(\lambda) = 1$ that means $\tau(\lambda) = \frac{1}{\lambda}$ and then $\tau(j) = j$. Since $\lambda, \mu \in \mathcal{O}_{L,S_L}^*$ we have that $\mathrm{ord}_{\mathfrak{B}}(\lambda^2 - \lambda + 1) \geq 0$ for all $\mathfrak{B} \notin S_L$ and then $j \in \mathcal{O}_{K,S}$. If $w \in K(S_K, 6)_{12}$ then by Proposition 2.1 there exists an elliptic curve over K with j -invariant equal to j and good reduction at all prime not in $S^{(6)}$. \square

4.3 $\mathrm{Gal}(L/K) \simeq C_3$

In case $\mathrm{Gal}(L/K) \simeq C_3$, the following theorem holds,

Theorem 4.2. *Let $\mathrm{Gal}(L/K) = \langle \sigma \rangle$. Suppose that $\Lambda \subset \mathcal{O}_{L,S_L}^*$ is associated with an elliptic curve defined over K . Then there exists $\lambda \in \Lambda$ satisfying the following conditions,*

⁵ $F_j(x)$ may not be irreducible. The crucial thing is that $F_j(x)$ has coefficients in K .

$$(i) \quad -\lambda \in \mathcal{O}_{L,K,S_L,1}^*.$$

$$(ii) \quad \sigma(\lambda) = \frac{1}{\mu}.$$

Conversely, let $\lambda \in \mathcal{O}_{L,S_L}^*$ and j, w, μ as above. If $\mu \in \mathcal{O}_{L,S_L}^*$ and (i)–(ii) hold then $j \in \mathcal{O}_{K,S}$. Moreover, if $w \in K(S, 6)_{12}$ then j is the j -invariant of an elliptic curve with good reduction outside $S^{(6)}$.

Proof. As in the quadratic case we can assume that $\sigma(\lambda) = S \cdot \lambda = \frac{1}{1-\lambda} = \frac{1}{\mu}$. Then an easy calculation shows that $N_{L/K}(-\lambda) = 1$. The proof of the converse is similar to Theorem (4.1). \square

From the condition $\sigma(\lambda) = \frac{1}{\mu}$ we also see that $N_{L/K}(-\mu) = 1$. Actually, one can prove that we can replace condition (ii) with the condition $-\mu \in \mathcal{O}_{L,K,S_L,1}^*$. As a result, we have that $\lambda, \mu \in \mathcal{O}_{L,K,S_L,\pm 1}^*$.

4.4 $\text{Gal}(L/K) \simeq S_3$

Finally, for the case $\text{Gal}(L/K) \simeq S_3$ we have similar result,

Theorem 4.3. *Let $\text{Gal}(L/K) = S_3 = \langle \sigma, \tau \rangle$ such that $\sigma^3 = \tau^2 = 1$. Suppose that $\Lambda \subset \mathcal{O}_{L,S_L}^*$ is associated with an elliptic curve defined over K . Then there exists $\lambda \in \Lambda$ satisfying the following conditions,*

$$(i) \quad \lambda \in \mathcal{O}_{L,L^\tau,S_L,1}^*.$$

$$(ii) \quad -\lambda \in \mathcal{O}_{L,L^\sigma,S_L,1}^*.$$

$$(iii) \quad \sigma(\lambda) = \frac{1}{\mu}.$$

Conversely, let $\lambda \in \mathcal{O}_{L,S_L}^*$ and j, w, μ as above. If $\mu \in \mathcal{O}_{L,S_L}^*$ and (i)–(iii) hold then $j \in \mathcal{O}_{K,S}$. Moreover, if $w \in K(S, 6)_{12}$ then j is the j -invariant of an elliptic curve with good reduction outside $S^{(6)}$.

Proof. As in the proofs of Theorems (4.1) and (4.2) we can assume that $\sigma(\lambda) = S \cdot \lambda = \frac{1}{1-\lambda} = \frac{1}{\mu}$ and $\tau(\lambda) = T \cdot \lambda = \frac{1}{\lambda}$. The last two equations show that $N_{L/L^\sigma}(-\lambda) = 1$ and $N_{L/L^\tau}(\lambda) = 1$, respectively. The proof of the converse is similar to theorem (4.1). \square

Since, we have proved that λ and μ are constrained to lie in different subgroups of \mathcal{O}_{L,S_L}^* we denote by G_λ and G_μ the groups where λ and μ lie. If M_L is the set of places of L then we define,

$$S_\lambda := \{\mathfrak{P} \in M_L : |x|_{\mathfrak{P}} \neq 1 \text{ for some } x \in G_\lambda\}$$

$$S_\mu := \{\mathfrak{P} \in M_L : |x|_{\mathfrak{P}} \neq 1 \text{ for some } x \in G_\mu\}$$

By the relation $\sigma(\lambda) = \frac{1}{\mu}$ in the C_3 and S_3 cases, we can make a choice of bases of G_λ and G_μ such that λ and μ have the same vector of exponents.

Since, solving S -unit equations it is the hardest part of the method, we want to avoid doing more computations than necessary. To complete this section we include

several results which in practice reduce the number of S -unit equations which need to be solved.

In the case where the initial set of primes S does not include a prime \mathfrak{p} above 2 the following two propositions hold,

Proposition 4.1. *If $[L : K] = 2, 3$ and E has good reduction at a prime $\mathfrak{p} \mid 2$ then $\text{ord}_{\mathfrak{p}}(\Delta(L/K)) \equiv 0 \pmod{2}$.*

Proof. There exists $k \in K^*$ such that $k^2\Delta(L/K) = \Delta(2^4f_2) = 2^{16}\Delta(f_2)$. By Lemma 3.1 in [CL07] we know that $\text{ord}_{\mathfrak{p}}(\Delta) \equiv 0 \pmod{12}$. Finally, using equation (3) we get the result. \square

Proposition 4.2. *If $[L : K] = 6$, L_c a cubic subfield and E has good reduction at a prime $\mathfrak{p} \mid 2$ then $\text{ord}_{\mathfrak{p}}(\Delta(L_c/K)) \equiv 0 \pmod{2}$.*

Proof. We know that there exists $k \in K^*$ such that $k^2\Delta(L_c/K) = \Delta(2^4f_2) = 2^{16}\Delta(f_2)$. The rest is as above. \square

Because finding isogenous curves is a quite fast procedure, in practice we also assume that we are looking for curves up to isogeny in order to reduce the number of S -unit equations we have to solve. When E has full two torsion we have,

Proposition 4.3. *If E has full two torsion then it is isogenous to one without full two torsion.*

Proof. See Proposition 2.1 of [Rib76]. \square

Proposition 4.3 actually says that we do not have to solve S -equations in the case $L = K$.

Let E/K be an elliptic curve with a rational 2-torsion point. We assume that E is of the following form,

$$E : y^2 = x(x^2 + ax + b), \text{ with } a, b \in \mathcal{O}_K$$

Then, the 2-isogenous of E is the curve

$$\bar{E} : Y^2 = X(X^2 + \bar{a}X + \bar{b})$$

where $\bar{a} = -2a$ and $\bar{b} = a^2 - 4b$. An easy calculation shows that $\Delta(E) = 2^4b^2(a^2 - 4b)$ and $\Delta(\bar{E}) = 2^4\bar{b}^2(\bar{a}^2 - 4\bar{b}) = 2^8b(a^2 - 4b)^2$.

Proposition 4.4. *Let E, \bar{E} be as above. If $(\frac{\cdot}{\cdot})_K$ is the Hilbert symbol relative to K then we have,*

$$\left(\frac{\Delta(E), \Delta(\bar{E})}{K} \right) = 1.$$

Proof. The equation $\Delta(E)x^2 + \Delta(\bar{E})y^2 = z^2$ has the non-trivial solution $(1, 2, a)$ in \mathcal{O}_K^3 . \square

The previous two propositions help us to reduce the number of S -unit equations we have to solve. If L is the 2-division field of an elliptic curve with only one rational point of order 2 then $\Delta(E) \equiv d \pmod{K^{*2}}$ where $L = K(\sqrt{d})$ for $d \in K(S_K, 2)$ by Proposition 3.1. We find the smallest set D of d 's such that at least one of the d_1, d_2 belongs in D when $\left(\frac{d_1, d_2}{K}\right) = 1$ for all possible combinations of d_1, d_2 (including the case $d_1 = d_2$). Then we have to solve the S -unit equation (2) only for the cases when $d \in D$ and then find all the isogenous curves.

5 Efficient Sieve

As we briefly explained in the introduction, the generalized S -unit algorithm to find all solutions of equation (2) where λ, μ lie in (possibly different) finitely generated subgroups of L^* for some number field L with generators $\lambda_0, \lambda_1, \dots, \lambda_n$ and $\mu_0, \mu_1, \dots, \mu_k$ has three main steps:

- (1) Use bounds of linear forms and p -adic logarithms to obtain bounds for the exponent vectors of λ, μ for any solutions.
- (2) Use lattice basis reduction algorithms and LLL-reduction to reduce these bounds as much as possible.
- (3) Use a sieve method to discard many candidate λ, μ which do not give solutions.

General sieve methods have been suggested by Smart and Wildanger ([Sma99], [Wil00]). However, we benefit from Theorems 4.1, 4.2 and 4.3 and the symmetries they introduce. We modify Smart and Wildanger's ideas avoiding the use of Finke-Pohst algorithm ([FP85]) in any point of the sieve as they suggest. By contrast with Smart and Wildanger we allow each generator to have its own upper bound for the absolute value of its exponent. Also it is important to mention that a choice of basis for G_λ and G_μ such that some of the generators are units (if it is possible) is crucial.

For the rest of this section we fix bases for G_λ and G_μ and we express λ and μ as a multiplicative combination of the bases,

$$\lambda = \prod_{i=0}^n \lambda_i^{x_i} \qquad \mu = \prod_{i=0}^m \mu_i^{y_i}$$

We always assume that λ_0 and μ_0 are the generators of the torsion part of G_λ and G_μ , respectively. We also assume that from steps (1) and (2) of the algorithm we have two vectors $B_0 = (b_0^0, b_1^0, \dots, b_n^0)$ and $C_0 = (c_0^0, c_1^0, \dots, c_m^0)$ such that for every solution, $|x_i| \leq b_i$ and $|y_j| \leq c_j$ for all $i = 0, \dots, n$ and $j = 0, \dots, m$.

For a fixed subset I of $\{0, 1, \dots, n\}$ we define

$$S_I = \{\mathfrak{B} \in S_\lambda : \exists \lambda_i \text{ with } i \in I \text{ such that } |\lambda_i|_{\mathfrak{B}} \neq 1\}.$$

$$\lambda_I = \prod_{i \in I} \lambda_i^{x_i}.$$

We denote by $I^\infty = \{i \in \{0, 1, \dots, n\} : \lambda_i \text{ is a unit}\}$ and $\lambda_\infty = \lambda_{I^\infty}$. Similarly, we define S_J for J a fixed subset of $\{0, 1, \dots, m\}$, J^∞ and μ_∞ . Since we use Theorems 4.1, 4.2 and 4.3, the sieve depends on $\text{Gal}(L/K)$.

C_2 case Let τ be the generator of $\text{Gal}(L/K)$. By the first part of Theorem 4.1 we understand that $G_\mu = \mathcal{O}_{L,S_L}^*$, and S_λ contains only split primes \mathfrak{B} such that $\text{ord}_{\mathfrak{B}}(g) = -\text{ord}_{\tau(\mathfrak{B})}(g)$ for all $g \in G_\lambda$. For each one of the conjugate finite primes $\mathfrak{B} \in S_\lambda$ we prove that there are no pairs of solutions (λ, μ) for which $|\text{ord}_{\mathfrak{B}}(\lambda)|$ is ‘large’. We do this by showing that,

$$|\mu - 1|_{\mathfrak{B}} < \delta \ll 1$$

has no non-trivial solutions, using Lemma 4 in [Sma99]. We use the new upper bounds on $|\text{ord}_{\mathfrak{B}}(\lambda)|$ obtained in this way to get new vectors $B_1 = (b_0^1, b_1^1, \dots, b_n^1)$ and $C_1 = (c_0^1, c_1^1, \dots, c_m^1)$.

Since we have chosen only finite primes $\mathfrak{B} \in S_\lambda$ we have not reduced the exponents bounds b_i^1 and c_j^1 for the unit generators. The way we reduce the bounds for the unit generators is to split the set of solutions in two sets, where the first set contains solutions with smaller exponents, and try to show that the second set contains no solutions. In order to do that we need a few definitions. Let $S_\lambda^\infty := S_{I^\infty}$ then⁶,

Definition 5.1. Let $B = (b_0, b_1, \dots, b_n) \in \mathbb{N}^{n+1}$ and $C = (c_0, c_1, \dots, c_n) \in \mathbb{N}^{m+1}$. Then for $R > 1$ we define,

$$\mathcal{L}_\infty^2(B, C, R) = \{(\lambda, \mu) : |x_i| \leq b_i, |y_i| \leq c_i \text{ and } |\log |\lambda|_{\mathfrak{B}}| \leq \log(R), \forall \mathfrak{B} \in S_\lambda^\infty\}.$$

Let

$$R_{1,\infty} := \max_{\mathfrak{B} \in S_\lambda^\infty} \exp \left(\sum_{i=1}^n b_i^1 |\log |\lambda_i|_{\mathfrak{B}}| \right).$$

Lemma 5.1. Every pair of solutions (λ, μ) lies in $\mathcal{L}_\infty^2(B_1, C_1, R_{1,\infty})$.

Proof. For a $\mathfrak{B} \in S_\lambda^\infty$ we have,

$$\begin{aligned} |\log |\lambda|_{\mathfrak{B}}| &\leq \sum_{i=1}^n x_i |\log |\lambda_i|_{\mathfrak{B}}| \leq \sum_{i=1}^n b_i^1 |\log |\lambda_i|_{\mathfrak{B}}| \\ &\leq \max_{\mathfrak{B} \in S_\lambda^\infty} \sum_{i=1}^n b_i^1 |\log |\lambda_i|_{\mathfrak{B}}| = \log(R_{1,\infty}). \end{aligned}$$

□

Definition 5.2. Let B and C be as above then for $\mathfrak{B} \in S_\lambda^\infty$ and $1 < R' < R$ we define,

$$T_{\mathfrak{B}}^2(B, C, R, R') = \left\{ (\lambda, \mu) \in \mathcal{L}_\infty^2(B, C, R) : \begin{array}{l} |\mu - 1|_{\mathfrak{B}} < \frac{1}{R'} \text{ or} \\ |\frac{\mu}{\lambda} - 1|_{\mathfrak{B}} < \frac{1}{R'} \end{array} \right\}.$$

We need the following lemma,

⁶Note that $\mathfrak{B} \in S_\lambda^\infty \Leftrightarrow \tau(\mathfrak{B}) \in S_\lambda^\infty$.

Lemma 5.2. *There is a computable constant $c_{1,\infty} > 0$ such that*

$$x_i \leq c_{1,\infty} \max_{\mathfrak{B} \in S_\lambda^\infty} (|\log |\lambda_\infty|_{\mathfrak{B}}|)$$

for all $i \in I^\infty$.

Proof. We may assume that $I^\infty = \{1, 2, \dots, t\}$ and $S_\lambda^\infty = \{\mathfrak{B}_1, \dots, \mathfrak{B}_u\}$ with $t \leq u$. We define the matrix

$$M = \begin{pmatrix} \log |\lambda_1|_{\mathfrak{B}_1} & \cdots & \log |\lambda_t|_{\mathfrak{B}_1} \\ \vdots & & \vdots \\ \log |\lambda_1|_{\mathfrak{B}_u} & \cdots & \log |\lambda_t|_{\mathfrak{B}_u} \end{pmatrix}$$

By the choice of I^∞ and S_λ^∞ there exists a $t \times t$ submatrix of M which is invertible. Among all these submatrices we pick one, which we call M_t , whose inverse has the maximal infinity norm. Define $c_{1,\infty} = \|M_t^{-1}\|_\infty$. Then we can deduce that $|x_i| \leq c_{1,\infty} \max_{\mathfrak{B} \in S_\lambda^\infty} (|\log |\lambda_\infty|_{\mathfrak{B}}|)$. \square

Proposition 5.1. *Let $1 < R_{k+1} < R_k$, and let B_k and C_k be vectors of the exponent bounds such that every solution (λ, μ) lies in $\mathcal{L}_\infty^2(B_k, C_k, R_k)$. Then,*

$$\mathcal{L}_\infty^2(B_k, C_k, R_k) = \mathcal{L}_\infty^2(B_{k+1}, C_{k+1}, R_{k+1}) \bigcup \bigcup_{\mathfrak{B} \in S_\lambda^\infty} T_{\mathfrak{B}}^2(B_k, C_k, R_k, R_{k+1})$$

where $C_{k+1} = C_k$, $b_i^{k+1} = \min(b_i^k, c_{1,\infty} \log(R_{k+1}) + c_{1,\infty} c_{2,\infty})$ for $i \in I^\infty$, otherwise $b_i^{k+1} = b_i^k$ and $c_{2,\infty} = \max_{\mathfrak{B} \in S_\lambda^\infty} \sum_{i \notin I^\infty} b_i^k |\log |\lambda_i|_{\mathfrak{B}}|$.

Proof. Let $(\lambda, \mu) \in \mathcal{L}_\infty^2(B_k, C_k, R_k)$ but $(\lambda, \mu) \notin \mathcal{L}_\infty^2(B_{k+1}, C_{k+1}, R_{k+1})$. That means there exists $\mathfrak{B} \in S_\lambda^\infty$ such that $|\lambda|_{\mathfrak{B}} > R_{k+1}$ or $|\lambda|_{\mathfrak{B}} < \frac{1}{R_{k+1}}$. In the first case we get that,

$$\begin{aligned} |\lambda|_{\mathfrak{B}} > R_{k+1} &\Leftrightarrow |\tau(\lambda)|_{\tau(\mathfrak{B})} > R_{k+1} \Leftrightarrow \\ \left| \frac{1}{\lambda} \right|_{\tau(\mathfrak{B})} < \frac{1}{R_{k+1}} &\Leftrightarrow \left| \frac{\mu}{\lambda} - 1 \right|_{\tau(\mathfrak{B})} < R_{k+1}. \end{aligned}$$

In the second case we get $|\lambda|_{\mathfrak{B}} < \frac{1}{R_{k+1}} \Leftrightarrow |\mu - 1|_{\mathfrak{B}} < \frac{1}{R_{k+1}}$. Finally, $(\lambda, \mu) \in T_{\mathfrak{B}}^2(B_k, C_k, R_k, R_{k+1})$ or $T_{\tau(\mathfrak{B})}^2(B_k, C_k, R_k, R_{k+1})$.

Now for $(\lambda, \mu) \in \mathcal{L}_\infty^2(B_k, C_k, R_{k+1})$ we have that

$$|\log |\lambda_\infty|_{\mathfrak{B}}| \leq |\log |\lambda|_{\mathfrak{B}}| + \left| \log \left| \frac{\lambda}{\lambda_\infty} \right|_{\mathfrak{B}} \right| < \log(R_{k+1}) + c_{2,\infty}$$

and by Lemma (5.2) we get,

$$x_i \leq c_{1,\infty} \log(R_{k+1}) + c_{1,\infty} c_{2,\infty}.$$

So, we deduce that $(\lambda, \mu) \in \mathcal{L}_\infty^2(B_{k+1}, C_{k+1}, R_{k+1})$. \square

Proposition 5.1 is very useful in practice because we can quickly prove when the set $T_{\mathfrak{B}}^2(B_k, C_k, R_k, R_{k+1})$ has non-trivial solutions or not. In paragraph 3.1 Lemma 3 of [Sma99] Smart shows how to do that. The only difference we have introduced, which does not change the construction, is that we allow different upper bounds for the exponents while they have for all the same bound. We leave to the reader to see how the proof of Lemma 3 in [Sma99] adapts to our case.

C_3 case Let σ be the generator of $\text{Gal}(L/K)$. We recall that we have chosen bases of G_λ and G_μ such that $n = m$ and $x_i = y_i$ for all $i = 0, \dots, n$ according to Theorem 4.2 by choosing $\mu_i = \sigma(\frac{1}{\lambda_i})$. So, we have to consider only one bound vector B_k at each step of the sieve. Also, we want to recall that $G_\lambda = G_\mu$ and as a result $S_\lambda = S_\mu$. By Theorem 4.2 we see that S_λ contains only split finite primes.

Again, as in the quadratic case, the first step is to find an upper bound on $|\text{ord}_{\mathfrak{B}}(\lambda)|$ for each $\mathfrak{B} \in S_\lambda$, by proving that,

$$|\mu - 1|_{\mathfrak{B}} < \delta \ll 1$$

has no non-trivial solutions. We use the new upper bounds of $|\text{ord}_{\mathfrak{B}}(\lambda)|$ to find a new bound vector B_1 .

Now, we want to reduce the bound for the unit generators. We observe that $I^\infty = J^\infty$.

Definition 5.3. Let $B = (b_0, b_1, \dots, b_n) \in \mathbb{N}^{n+1}$. Then for $R > 1$ we define,

$$\mathcal{L}_\infty^3(B, R) = \{(\lambda, \mu) : |x_i| \leq b_i \text{ and } |\log |\lambda|_{\mathfrak{B}}| \leq \log(R), \forall \mathfrak{B} \in S_\lambda^\infty\}.$$

Lemma 5.3. Every pair of solutions (λ, μ) lies in $\mathcal{L}_\infty^3(B_1, R_{1,\infty})$ with $R_{1,\infty}$ as above.

Proof. Similar to the quadratic case, Lemma 5.1. \square

Definition 5.4. Let B be as above, then for each $\mathfrak{B} \in S_\lambda^\infty$ and $1 < R' < R$ we define,

$$T_{\mathfrak{B}}^3(B, R, R') = \left\{ (\lambda, \mu) \in \mathcal{L}_\infty^3(B, R) : \begin{array}{l} |\mu - 1|_{\mathfrak{B}} < \frac{1}{R'} \text{ or} \\ |\lambda - 1|_{\sigma(\mathfrak{B})} < \frac{1}{R'} \end{array} \right\}.$$

If $c_{1,\infty}$ is as in Lemma 5.2 then, we have:

Proposition 5.2. Let $1 < R_{k+1} < R_k$ and B_k be bound vector of the exponents. Then,

$$\mathcal{L}_\infty^3(B_k, R_k) = \mathcal{L}_\infty^3(B_{k+1}, R_{k+1}) \cup \bigcup_{\mathfrak{B} \in S_\lambda^\infty} T_{\mathfrak{B}}^3(B_k, R_k, R_{k+1})$$

where $b_i^{k+1} = \min(b_i^k, c_{1,\infty} \log(R_{k+1}) + c_{1,\infty} c_{2,\infty})$ for $i \in I^\infty$ otherwise $b_i^{k+1} = b_i^k$ and $c_{2,\infty} = \max_{\mathfrak{B} \in S_\lambda^\infty} \sum_{i \notin I^\infty} b_i^k |\log |\lambda_i|_{\mathfrak{B}}|$.

Proof. Similar to Proposition 5.1. \square

S_3 case As above let $\text{Gal}(L/K) = \langle \sigma, \tau \rangle$ where $\sigma^3 = \tau^2 = 1$ and $\tau\sigma\tau = \sigma^2$. As in the cubic case we may choose bases of G_λ and G_μ such that $n = m$ and $x_i = y_i$ for all $i = 0, \dots, n$ using Theorem 4.3 and choosing $\mu_i = \sigma(\frac{1}{\lambda_i})$. Again, we have only to consider only one bound vector B_k and we have $I^\infty = J^\infty$. However, we may now have $G_\lambda \neq G_\mu$ and $S_\lambda \neq S_\mu$. We define $S_\mu^\infty = S_{J^\infty}$.

Again, the first step is to find an upper bound of $|\text{ord}_{\mathfrak{B}}(\lambda)|$ for each $\mathfrak{B} \in S_\lambda$ by proving that,

$$|\mu - 1|_{\mathfrak{B}} < \delta \ll 1$$

has no non-trivial solutions. We use the new upper bounds of $|\text{ord}_{\mathfrak{B}}(\lambda)|$ to get new bounds B_1 .

Definition 5.5. Let $B = (b_0, b_1, \dots, b_n) \in \mathbb{N}^{n+1}$. Then for $R > 1$ we define,

$$\mathcal{L}_\infty^6(B, R) = \left\{ (\lambda, \mu) : |x_i| \leq b_i \text{ and } \begin{array}{l} |\log |\lambda|_{\mathfrak{B}}| \leq \log(R) \\ |\log |\mu|_{\mathfrak{B}}| \leq \log(R) \end{array}, \forall \mathfrak{B} \in S_\lambda^\infty \cup S_\mu^\infty \right\}.$$

Lemma 5.4. Every pair of solutions (λ, μ) lies in $\mathcal{L}_\infty^6(B_1, R_{1,\infty})$ with $c_{1,\infty}$ and $R_{1,\infty}$ as above.

Proof. Similar to lemma 5.1. □

Definition 5.6. Let B be as above. Then for each $\mathfrak{B} \in S_\lambda^\infty \cup S_\mu^\infty$ and $1 < R' < R$ we define,

$$T_{\mathfrak{B}}^6(B, R, R') = \left\{ (\lambda, \mu) \in \mathcal{L}_\infty^6(B, R) : \begin{array}{l} |\mu - 1|_{\mathfrak{B}} < \frac{1}{R'} \text{ or} \\ |\lambda - 1|_{\mathfrak{B}} < \frac{1}{R'} \text{ or} \\ |\mu - 1|_{\sigma^2(\mathfrak{B})} < \frac{1}{R'} \text{ or} \\ |\lambda - 1|_{\sigma(\mathfrak{B})} < \frac{1}{R'} \end{array} \right\}.$$

The following proposition is proved in the same way as Proposition 5.2,

Proposition 5.3. Let $1 < R_{k+1} < R_k$ and B_k be bound vector of the exponents. Then it holds,

$$\mathcal{L}_\infty^6(B_k, R_k) = \mathcal{L}_\infty^6(B_{k+1}, R_{k+1}) \cup \bigcup_{\mathfrak{B} \in S_\lambda^\infty \cup S_\mu^\infty} T_{\mathfrak{B}}^6(B_k, R_k, R_{k+1})$$

where $b_i^{k+1} = \min(b_i^k, c_{1,\infty} \log(R_{k+1}) + c_{1,\infty} c_{2,\infty})$ for $i \in I^\infty$ otherwise $b_i^{k+1} = b_i^k$ and $c_{2,\infty} = \max_{\mathfrak{B} \in S_\lambda^\infty} \sum_{i \notin I^\infty} b_i^k |\log |\lambda_i|_{\mathfrak{B}}|$.

We should mention that in this case it may happen that there exists $\mathfrak{B} \in S_\lambda^\infty \cup S_\mu^\infty$ such that $\text{ord}_{\mathfrak{B}}(\lambda) = 0$. Then we can not use Lemma 3 in [Sma99] to prove that the inequality $|\lambda - 1|_{\mathfrak{B}} < \frac{1}{R_{k+1}}$ does not contain non-trivial solutions. However, for such a solution we have $|\log |\lambda|_{\mathfrak{B}}| = 0$ and $|\log |\mu|_{\mathfrak{B}}| \leq \log(R_{k+1})$ and if it does not lie in any set $T_{\mathfrak{B}}^6(B_k, R_k, R_{k+1})$ then it has to be in $\mathcal{L}_\infty^6(B_{k+1}, R_{k+1})$.

If we continue this way we reach to a point where we are not able to prove that the sets $T_{\mathfrak{B}}^i$ do not contain non-trivial solutions. If the bounds and the rank of the groups are small we can just do a simple loop to find all solutions, using these bounds.

However, we may still have a lot of cases to check. The idea is to find all the solutions such that $\lambda \equiv 1 \pmod{\mathfrak{B}^e}$ for all finite primes in $\mathfrak{B} \in S_\mu$ and suitable (small) choice of e . Now, we know that the remaining solutions have smaller valuation for all finite primes, and we can deduce smaller bounds for the non-unit generators of G_λ and G_μ . Since we have smaller upper bounds for the non-unit generators, we can apply all the above results to reduce smaller bounds for the unit generators.

We can repeat the above procedure up to the point where a simple loop is feasible. In the C_3 and S_3 cases we also use general Hilbert symbols to reduce the number of cases we have to check in the final loop. Our solutions (λ, μ) always satisfy $\left(\frac{\lambda\mu}{\mathfrak{B}}\right)_\ell$ for every prime \mathfrak{B} and integer $\ell \geq 1$. For a suitable choice⁷ of \mathfrak{B} and ℓ we create the matrix $A_{\mathfrak{B}} = \left(\left(\frac{\lambda_i\mu_j}{\mathfrak{B}}\right)_\ell\right)_{i,j} \in \mathbb{M}_{n+1,n+1}(\mathbb{Z}/\ell\mathbb{Z})$ and we test whether $xA_{\mathfrak{B}}x^t = 0$.

In practice, it seems that we have to solve $\lambda \equiv 1 \pmod{\mathfrak{B}^e}$ just once. However, there are cases where trying to find the solution of $\lambda \equiv 1 \pmod{\mathfrak{B}^e}$ it is the most expensive part.

6 Examples

For reasons of space we cannot include the full details of the results obtained here; complete lists of the join variants in each case may be found at the author's web page <http://www2.warwick.ac.uk/fac/sci/maths/people/staff/koutsianas>.

We have compared our results with Cremona's and LMFDB's database[LMF15]. Finally, we have to say that all the computations have been done in the servers at Mathematics Institute of University of Warwick and all the code has been written in Sage[Dev15].

6.1 $K = \mathbb{Q}$

As in [CL07] we have computed all the curves for set of primes $S = \{2\}, \{2, 3\}$ and $\{2, p\}$ for $p = 3, \dots, 23$. We present a couple of examples in order to compare our method with the Cremona–Lingham method. We also give an example with $S = \{2, 3, 23\}$ which seems to be beyond the range of the Cremona–Lingham method.

Case $S = \{2, 3\}$ We found 83 j -invariants as in [CL07]. We solved 3 S -unit equations for the C_2 case, one S -unit equation for the C_3 case and 8 S -unit equations for the S_3 . In all these cases we had no difficulties in the reduction and sieve steps. However, it seems that the Cremona–Lingham method works faster because we have the large number of S -unit equations to solve in the S_3 case.

Case $S = \{2, 17\}$ For this set of primes we did not have the difficulties as in [CL07] where they had to evaluate generators of the Mordell-Weil group with huge denominators of the x -coordinate using Heegner points. We only had to solve 3 S -unit

⁷We use tame Hilbert symbols because there are formulas to evaluate it which are easy implement compared to the general case. That means we choose only primes in $S_\lambda \cup S_\mu$ and choose ℓ to be the order of the unit group of the residue field at \mathfrak{B} .

equations over the quadratic fields $\mathbb{Q}(\sqrt{17})$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{34})$. We found 29 j -invariants.

It would be very useful if we could benefit in Cremona–Lingham method by the fact that we had to solve S -unit equations only for these 3 quadratic fields. So far, we can not see how we could combine the two methods.

Case $S = \{2, 3, 23\}$ We had to solve S -unit equations for 8 quadratic fields, 1 cubic extension and 37 S_3 extensions. We found 311 isomorphism classes of curves and 5504 curves. We got curves with the possible maximal conductor $2^8 3^5 23^2 = 32908032$ which is beyond the range of the current modular symbol method [Cre97]. Moreover, in Cremona–Lingham method there were cases where the Mordell–Weil groups could not be computed. It worthy to mention that the most expensive part of the computation was the sieve for the only one S_3 case with $\text{rank}(G_\lambda) = 4$. It took around 6 times more than all the other computations we had.

More computations Apart from the sets of primes S we presented above, we have computed all the curves for the following set of primes,

- Curves with at least one rational 2-torsion point for the set of primes $S = \{p\}$ for $p \leq 200$, $S = \{p, q\}$ for $p \leq 11$ and $q \leq 200$, $S = \{2, 3, p\}$ for $p \leq 43$ and $S = \{2, 5, p\}$ for $p \leq 37$.
- Curves with cubic 2-division field for $S = \{p\}$ for $p \leq 200$, $S = \{p, q\}$ for $p \leq 5$ and $q \leq 200$, $S = \{7, p\}$ for $p \leq 29$ and $S = \{2, 3, p\}$ for $p \leq 41$.
- Curves with S_3 2-division field for $S = \{p\}$ for $p \leq 181$ and $S = \{2, p\}$ for $p \leq 127$.

From the computations we have done and the current implementation, it seems that the method works well when the set S does not have very many number of primes and the primes are not too big. For example, it seems impossible to us to do computations with primes with 4, 5 or more digits. Even the calculation of S -unit groups over quadratic fields becomes difficult in this case.

6.2 Quadratic fields

6.2.1 $K = \mathbb{Q}(\sqrt{-1})$

Case $S = \{p|2\}$ We found 17 j -invariants and 64 curves. We had to solve 3 S -unit equations for quadratic extensions of K . We get the same number of j -invariants and curves as in [Las83].

6.2.2 $K = \mathbb{Q}(\sqrt{5})$

Case $S = \{p|31\}$ For this case we only have partial results. We have computed all the curves with at least one rational 2-torsion point. We have found 12 j -invariants and 24 curves. We solved S -unit equations for 7 quadratic extensions of K .

References

- [CL07] J. E. Cremona and M. P. Lingham. Finding All Elliptic Curves with Good Reduction Outside a Given Set of Primes. *Experimental Mathematics*, 16(3):303–312, 2007.
- [Coh96] H. Cohen. *A Course in Computational Algebraic Number Theory*. Number 138 in Graduate Texts in Mathematics. Springer-Verlag, New York, 1996.
- [Coh99] H. Cohen. *Advanced Topics in Computational Number Theory*. Number 193 in Graduate Texts in Mathematics. Springer-Verlag, New York, 1999.
- [Cre97] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.
- [Dev15] The Sage Developers. *Sage Mathematics Software (Version 6.8)*, 2015. <http://www.sagemath.org>.
- [FP85] U. Fincke and M. Pohst. Improved Methods for Calculating Vectors of Short Length in a Lattice, Including a Complexity Analysis. *Mathematics of Computation*, 44(170):463–471, 1985.
- [Kid01a] M. Kida. Computing elliptic curves having good reduction everywhere over quadratic fields. *Tokyo J. Math.*, 24(2):545–558, 2001.
- [Kid01b] M. Kida. Good reduction of elliptic curves over imaginary quadratic fields. *J. Theor. Nombres Bordeaux*, 13(1):201–209, 2001.
- [Las83] Michael Laska. *Elliptic curves over number fields with prescribed reduction type*. Aspects of Mathematics, E4. Friedr. Vieweg & Sohn, Braunschweig; distributed by Heyden & Son, Inc., Philadelphia, PA, 1983.
- [LMF15] The LMFDB Collaboration. The L-functions and Modular Forms Database. <http://www.lmfdb.org>, 2015. [Online; accessed 12 November 2015].
- [Rib76] Kenneth A. Ribet. A modular construction of unramified p -extensions of $\mathbb{Q}(\mu_p)$. *Invent. Math.*, 34(3):151–162, 1976.
- [Sil08] J. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate text in mathematics*. Springer-Verlag, New York, 2 edition, 2008.
- [Sma95] N. P. Smart. The solution of triangularly connected decomposable form equations. *Mathematics of Computation*, 64(210):819–840, 1995.
- [Sma98] N. P. Smart. *The Algorithmic Resolution of Diophantine Equations*. Number 41 in Students Texts. London Mathematical Society, 1998.
- [Sma99] N. P. Smart. Determining the Small Solutions to S-unit Equations. *Mathematics of Computation*, 68(228):1687–1699, 1999.
- [TW89] N. Tzanakis and B. M. M. De Weger. On the Practical Solution of the Thue Equation. *Journal of Number Theory*, 31:99–132, 1989.

- [TW91] N. Tzanakis and B. M. M. De Weger. Solving a specific Thue-Mahler equation. *Mathematics of Computation*, 57(196):799–815, 1991.
- [TW92] N. Tzanakis and B. M. M. De Weger. How to explicitly solve a Thue-Mahler equation. *Compositio Mathematica*, 84(3):223–288, 1992.
- [Weg87] B. M. M. De Weger. Solving Exponential Diophantine Equations Using Lattice Basis Reduction Algorithm. *Journal of Number Theory*, 26:325–367, 1987.
- [Weg88] B. M. M. De Weger. *Algorithms For Diophantine Equations*. PhD thesis, University of Leiden, 1988.
- [Wil00] K. Wildanger. Solving unit and index form equations in algebraic number fields. *Journal of Number Theory*, 82:188–224, 2000.

MATHEMATICS INSTITUTE, UNIVERSITY OF WARWICK, COVENTRY, UK

E-mail address, A. Koutsianas: `a.koutsianas@warwick.ac.uk`